UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/495,509	02/01/2000	Robert Karch	125/1	4954

7590   10/11/2005

Kaplan & Gilman LLP
900 Route 9 North
Woodbridge, NJ 07095

EXAMINER
DAVIS, ZACHARY A

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/495,509	KARCH, ROBERT
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>01 August 2005</u>.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-20 and 22-47</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-20 and 22-47</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   An amendment was received on 01 August 2005. Claim 8 has been amended.

No claims have been added or canceled. Claims 1-20 and 22-47 are currently pending

in the present application.

Response to Arguments

2.   Applicant's arguments filed 01 August 2005 have been fully considered but they

are not persuasive.

Claims 1-20 and 22-47 were rejected under 35 U.S.C. 103(a). Specifically,

Claims 1-9, 30, 32, 33, 36, 37, 40-42, 45, and 46 were rejected as unpatentable over

Geiger et al, US Patent 6073142, in view of Sandhu, "Transaction Control Expressions

for Separation of Duties" (herein referred to as "Sandhu I") and Hudson et al, US Patent

6055637. Claim 16 was rejected as unpatentable over Geiger in view of Sandhu I and

Hudson and further in view of Scannell et al, US Patent 5377354. Claims 10, 13-15, 17,

18, 23, 24, 26, 27, 31, 34, 35, 43, and 47 were rejected under as unpatentable over

Geiger in view of Sandhu, "Lattice-Based Access Control Models" (herein referred to as

"Sandhu II") and Hudson. Claims 11, 12, 19, 20, 22, 25, 28, 29, 38, 39, and 44 were

rejected as unpatentable over Geiger in view of Sandhu II and Hudson and further in

view of Scannell.

In reference to independent Claims 1 and 8, Applicant argues that Sandhu I does not disclose a conditional rule, and that Sandhu I specifically does not disclose a rule precluding actions upon the occurrence of a condition. The Examiner respectfully disagrees. The Examiner believes that Sandhu I clearly states that the rules preclude certain actions depending on conditions (see page 282, column 2, where in step 3, the check must be issued by a different clerk). On page 283, top of column 2, the condition of Tom preparing a check precludes Tom from being the clerk who also issues the check. "If Tom attempts to issue that check ... the system *rejects the attempt*" (emphasis added). Because the attempt is rejected, the action is clearly precluded based on the condition. The Examiner further notes that the example of parties preparing, approving, and issuing checks described in Sandhu I (throughout the document, for example at pages 282-283, section 2, "Transactions") is analogous to the example described in the background of the present application (page 1, lines 21-26 and page 2, lines 5-12 of the present specification).

In reference to independent Claim 10, Applicant argues that there is no motivation or suggestion to combine the references. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21

USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation was as stated in the

previous Office action, namely to maintain the integrity of the security system (see

Hudson, column 1, lines 42-56). Further, one would be motivated to combine the

reference in order increase efficiency by not requiring updates (see Hudson, column 4,

lines 15-21). Applicant further argues that the claimed limitation of placing a rule

precluding an action upon occurrence of a condition into the management software after

the occurrence of the condition does not solve the integrity problem of Hudson but

rather improves efficiency. In response to this argument, the fact that applicant has

recognized another advantage which would flow naturally from following the suggestion

of the prior art cannot be the basis for patentability when the differences would

otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter.

1985).

In response to applicant's arguments against the references individually, one

cannot show nonobviousness by attacking references individually where the rejections

are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208

USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir.

1986). Specifically, Applicant attempts to draw the Examiner's attention to the fact that

Hudson only discloses rules that permit actions based on a condition, and not rules that

preclude actions based on a condition. However, this argument is spurious, as Hudson

was not relied upon to teach such a limitation. The Examiner notes that Sandhu I and

Sandhu II have been shown to teach rules that preclude actions based on a condition in

order to implement policies of a separation of duties and a Chinese Wall, respectively,

and that Hudson was instead relied upon for the more general teaching of including

dynamic generation of security rules, in general, in response to a condition occurring.

Therefore, for the reasons detailed above, the Examiner maintains the rejections

as set forth below.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

4.   Claims 1-9, 30, 32, 33, 36, 37, 40-42, 45, and 46 are rejected under 35 U.S.C.

103(a) as being unpatentable over Geiger et al, US Patent 6073142, in view of Sandhu,

"Transaction Control Expressions for Separation of Duties", hereinafter "Sandhu I", and

Hudson et al, US Patent 6055637.

In reference to Claims 1, 2, and 7, Geiger discloses a method using a database

of rules to implement organizational policies (column 3, lines 28-30) acting on various

data objects, including database records and information (column 2, lines 56-67 and

column 12, lines 35-45). Geiger describes the construction of rules (column 12, line 52-

column 17, line 2). More specifically, "Each rule describes a specific action to be taken

when an attribute of a ... data object satisfies an operator with respect to a user-defined

value" (column 13, lines 18-21). However, Geiger does not give examples of a rule

used to specifically preclude a second action upon the occurrence of a first action
defined as a condition, nor does Geiger use the specific example of separation of duties
as an organizational policy.

Sandhu I teaches that "Separation of duties is a fundamental technique for
prevention of fraud and errors" (pg. 282, column 1). An example of separation of duties
is given wherein a check is prepared by a clerk, the check is approved by a supervisor,
and the check is issued by a second clerk. This is done to ensure that "different users
have responsibility and authorization" for each step of the process (pg 282, column 2).
The separation of duties means that, in this example, "it will take collusion of two clerks
and a supervisor to perpetrate fraud" (pg 283, column 1) whereas, without separation of
duties, a single person would be more able to commit fraud. The example of preparing,
approving, and issuing a check is analogous to Claim 7, wherein the rule that is stored
and utilized in the system prevents the same user from both ordering goods or services
(a preliminary step to preparing the check) and paying for the goods or services
(approving and issuing the check). These benefits of the separation of duties are well
known, and it would be obvious to automate the enforcement of this policy once the
remainder of the system has been automated.

Therefore, it would have been obvious to one of ordinary skill in the art at the
time the invention was made to modify the method of Geiger by using its system of rules
to automate an implementation of a policy of separation of duties, as described by
Sandhu I, in order to prevent fraud and errors (see Sandhu I, pg. 282). However,

neither Geiger nor Sandhu I explicitly teach loading a rule into the software dynamically

upon the occurrence of the condition.

Hudson discloses a method for implementing varying security policies that

includes a temporary token that includes security rules (column 3, lines 61-63). Hudson

further discloses that these rules are dynamically generated upon the occurrence of a

condition (column 4, lies 10-15, where the rule is generated upon a user request for

access). Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to modify the method of Geiger and Sandhu I by including

dynamic generation of rules in response to the condition, in order to maintain the

integrity of the security systems (see Hudson, column 1, lines 42-56) and in order

increase efficiency by not requiring updates (see Hudson, column 4, lines 15-21).

In reference to Claim 5, Hudson further discloses that the rule is eliminated from

the software when the condition is rescinded (column 4, lines 15-21).

In reference to Claim 6, Geiger discloses that, upon returning a message to a

user, the user is notified, via email, of the reason that the message was returned

(column 16, lines 10-15).

In reference to Claims 3 and 4, Sandhu I discloses a further limitation for

separation of duties: once an action has been performed by one user, a second action

can only be performed by certain other users. Specifically, for the example of

preparing, approving, and issuing a check, after a clerk has prepared the check, only a

supervisor may approve the check. Similarly, once the supervisor has approved the

check, only a second clerk may issue the check. If a clerk attempts to approve the

check, or a supervisor attempts to approve the check, then the system should reject the attempt (page 283, columns 1-2). Specifically in reference to Claim 4, in the example described, the roles of the two users are different, specifically supervisor and clerk.

In reference to Claim 36, it would be obvious not to load a rule until a user in the role specified by the rule logs on in order to conserve system memory resources by not loading the rule unnecessarily.

Similarly, in reference to Claim 37, it would be obvious only to test a rule for a user in the role specified by the rule, in order to conserve processing resources by not testing the rule unnecessarily.

In reference to Claim 32, it would be obvious not to load a rule until a user specified by the rule logs on in order to conserve system memory resources by not loading the rule unnecessarily.

In reference to Claim 33, it would be obvious only to test a rule for a user specified by the rule, in order to conserve processing resources by not testing the rule unnecessarily.

In reference to Claim 40, the security policy is separation of duties, as described above in reference to Claim 1.

In reference to Claim 41, compliance to regulation is generally a legal requirement for the company administering such a system. It would be obvious to modify the combined system of Geiger and Sandhu I, described in reference to Claim 1, to include a policy of compliance to regulation in order to avoid the legal repercussions of a failure to comply.

Further, in reference to Claim 42, the benefits or requirements of privacy of data are well known. It would be obvious to modify the combined system of Geiger and Sandhu I, described in reference to Claim 1, to include a policy of privacy of data in order to gain the benefits of privacy.

In reference to Claim 45, Hudson further discloses generating rules in response to a condition (column 4, lies 10-15, where the rule is generated upon a user request for access).

In reference to Claim 8, Geiger discloses a system that includes a file of rules (Figure 2, Rule Base 270, and Figure 3, Gatekeeping Rule Base 289) and means for reading said file, locating said rules, and integrating said rules into the system (Figure 2, Rule Engine 210, and Figure 3, Rule Engine 283). However, Geiger does not give examples of rules used to prevent a specified data transaction by a user after a user has effected a specified transaction to modify data.

Sandhu I teaches that "Separation of duties is a fundamental technique for prevention of fraud and errors" (pg. 282, column 1). An example of separation of duties is given where the same individual cannot be responsible for preparing, approving, and issuing a check, as described with reference to Claims 1, 2, and 7 above. The benefits of the separation of duties are well known, and it would be obvious to automate the enforcement of this policy once the remainder of the system has been automated.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Geiger by using its system of rules

to automate an implementation of a policy of separation of duties, as described by

Sandhu I, in order to prevent fraud and errors (see Sandhu I, pg. 282). However,

neither Geiger nor Sandhu I explicitly teach integrating a rule into the software

dynamically upon the occurrence of a specified action.

Hudson discloses a method for implementing varying security policies that

includes a temporary token that includes security rules (column 3, lines 61-63). Hudson

further discloses that these rules are dynamically generated upon the occurrence of a

specified action (column 4, lies 10-15, where the rule is generated upon a user request

for access). Therefore, it would have been obvious to one of ordinary skill in the art at

the time the invention was made to modify the system of Geiger and Sandhu I by

including dynamic generation of rules in response to the action, in order to maintain the

integrity of the security systems (see Hudson, column 1, lines 42-56) and in order

increase efficiency by not requiring updates (see Hudson, column 4, lines 15-21).

In reference to Claim 9, Hudson further discloses that the rule is eliminated from

the software when the condition is rescinded (column 4, lines 15-21).

In reference to Claim 30, Sandhu I describes that a history of the objects acted

upon is created (pg 283, column 2) and that separation of duties can be enforced by

keeping such history information (pg 284, column 2). Geiger discloses that the rules

may be stored "by any of a number of useful implementing data structures" (column 16,

lines 42-45). Further, it would be obvious to store eliminated rules for record-keeping

purposes, and also in the event that a rule might need to be re-used.

In reference to Claim 46, Hudson further discloses generating rules in response to a specified user action (column 4, lies 10-15, where the rule is generated upon a user request for access).

5.   Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Geiger in view of Sandhu I and Hudson as applied to claim 1 above, and further in view of Scannell et al, US Patent 5377354.

In reference to Claim 16, Scannell discloses that a rule can be used as a template for other rules, in order to create a "new but similar rule" (column 8, lines 41-44). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined system of Geiger, Sandhu I, and Hudson, as described above in reference to Claim 1, by allowing for the use of templates for rule creation, in order to create "new but similar" rules, as taught by Scannell (see Scannell, column 8, lines 41-44).

6.   Claims 10, 13-15, 17, 18, 23, 24, 26, 27, 31, 34, 35, 43, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Geiger, US Patent 6073142, in view of Sandhu, "Lattice-Based Access Control Models", hereinafter "Sandhu II", and Hudson et al, US Patent 6055637.

In reference to Claim 10, Geiger discloses a system in which rules are stored (Figure 2, Rule Base 270, and Figure 3, Gatekeeping Rule Base 289) and included in the system (Figure 2, Rule Engine 210, and Figure 3, Rule Engine 283). However,

Geiger does not give examples of rules used to prevent a known party from accessing information on the condition that the party has knowledge of a particular set of information.

Sandhu II teaches that the objective of a Chinese Wall policy "is to prevent information flows that result in a conflict of interest for individual consultants" (pg. 17, column 2). For example, a consultant should not have access to information about two companies of the same type, such as two banks, "because such information creates a conflict of interest in the consultant's analysis and is a disservice to clients" (pg. 17, column 2). After a consultant has accessed information about one bank, the consultant is prevented from accessing information about another bank. Further, this prevention of access can be removed once information is no longer sensitive, but "should persist long enough to avoid a conflict of interest" (pg. 17, column 3).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Geiger by using its system of rules to automate an implementation of a Chinese Wall policy, as described by Sandhu II, in order to prevent a conflict of interest (see Sandhu II, pg. 17). However, neither Geiger nor Sandhu II explicitly teach loading a rule into the software dynamically upon the occurrence of a first condition or removing the rule from the software upon the occurrence of a second condition.

Hudson discloses a method for implementing varying security policies that includes a temporary token that includes security rules (column 3, lines 61-63). Hudson further discloses that these rules are dynamically generated upon the occurrence of a

first condition (column 4, lies 10-15, where the rule is generated upon a user request for access) and that the rule is eliminated from the software upon the occurrence of a second condition (column 4, lines 15-21). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Geiger and Sandhu II by including dynamic generation and removal of rules in response to the conditions, in order to maintain the integrity of the security systems (see Hudson, column 1, lines 42-56) and in order increase efficiency by not requiring updates (see Hudson, column 4, lines 15-21).

In reference to Claims 13 and 14, Geiger discloses that, upon returning a message to a user, the user is notified, via email, of the reason that the message was returned (column 16, lines 10-15).

In reference to Claim 15, it is well known that if information has been made public, it is no longer sensitive. Further, Sandhu II describes that the denial of access to information "should persist long enough to avoid a conflict of interest" (pg 17, column 3), that is, after a predetermined time, the information would no longer be considered sensitive.

In reference to Claim 17, Geiger discloses that messages may be sent to a "gatekeeper" for further review, if certain conditions are met and certain rules apply (see Abstract; Figures 1,3, 4A, and 4B; and column 3, lines 9-19, for example).

In reference to Claim 18, Geiger further discloses that, upon returning a message to a user, the user is notified, via email, of the reason that the message was returned (column 16, lines 10-15).

In reference to Claims 23, 24, 26, 27, and 43, Geiger discloses that messages

may be sent to a "gatekeeper" for further review, if certain conditions are met and

certain rules apply (see Abstract; Figures 1,3, 4A, and 4B; and column 3, lines 9-19, for

example). Specifically in reference to Claims 23 and 24, Geiger discloses that the

gatekeeper is notified, via email, of the reason that the message was sent on to the

gatekeeper (column 16, lines 10-15). Further, Geiger discloses that a message may be

sent on to another employee if a message matches certain properties (column 3, lines

53-61). Specifically in reference to Claims 26 and 27, Geiger discloses that a message

may be forwarded to a specific individual based on matching certain properties (column

3, lines 53-61, and column 7, Table 7, for example) where this could be the user's

manager or an employee responsible for data security. Specifically in reference to

Claim 43, Geiger discloses that the gatekeeping function may be an automated

computer process (column 24, lines 6-14).

In reference to Claim 31, Geiger discloses that the rules may be stored "by any of

a number of useful implementing data structures" (column 16, lines 42-45). Further, it

would be obvious to store eliminated rules for record-keeping purposes, and also in the

event that a rule might need to be re-used.

In reference to Claim 34, it would be obvious not to load a rule until a user

specified by the rule logs on in order to conserve system memory resources by not

loading the rule unnecessarily.

In reference to Claim 35, it would be obvious only to test a rule for a user specified by the rule, in order to conserve processing resources by not testing the rule unnecessarily.

In reference to Claim 47, Hudson further discloses generating rules in response to a first condition (column 4, lies 10-15, where the rule is generated upon a user request for access).

7.   Claims 11, 12, 19, 20, 22, 25, 28, 29, 38, 39, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Geiger in view of Sandhu II and Hudson as applied to claim 10 above, and further in view of Scannell et al, US Patent 5377354.

In reference to Claim 11, Scannell discloses that a rule can be used as a template for other rules, in order to create a "new but similar rule" (column 8, lines 41-44). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined system of Geiger, Sandhu II, and Hudson, as described above in reference to Claim 10, by allowing for the use of templates for rule creation, in order to create "new but similar" rules, as taught by Scannell (see Scannell, column 8, lines 41-44).

In reference to Claim 12, a party known to the system will in general be assigned a predetermined role; for example, Sandhu II describes users in a consultant role (pg. 17, column 2).

In reference to Claim 38, it would be obvious not to load a rule until a user in the role specified by the rule logs on in order to conserve system memory resources by not loading the rule unnecessarily.

Similarly, in reference to Claim 39, it would be obvious only to test a rule for a user in the role specified by the rule, in order to conserve processing resources by not testing the rule unnecessarily.

In reference to Claim 19, Geiger discloses that messages may be sent to a "gatekeeper" for further review, if certain conditions are met and certain rules apply (see Abstract; Figures 1,3, 4A, and 4B; and column 3, lines 9-19, for example).

In reference to Claim 20, Geiger further discloses that, upon returning a message to a user, the user is notified, via email, of the reason that the message was returned (column 16, lines 10-15).

In reference to Claims 22, 25, 28, 29, and 44, Geiger discloses that messages may be sent to a "gatekeeper" for further review, if certain conditions are met and certain rules apply (see Abstract; Figures 1,3, 4A, and 4B; and column 3, lines 9-19, for example). Specifically in reference to Claims 22 and 25, Geiger discloses that the gatekeeper is notified, via email, of the reason that the message was sent on to the gatekeeper (column 16, lines 10-15). Further, Geiger discloses that a message may be sent on to another employee if a message matches certain properties (column 3, lines 53-61). Specifically in reference to Claims 28 and 29, Geiger discloses that a message may be forwarded to a specific individual based on matching certain properties (column 3, lines 53-61, and column 7, Table 7, for example) where this could be the user's

manager or an employee responsible for data security. Specifically in reference to Claim 44, Geiger discloses that the gatekeeping function may be an automated computer process (column 24, lines 6-14).

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is 571-

273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER